

# **The Integrated Distributed Virtual Research Network: An Introduction**

**by Colleen Adams**

**ARL-TR-6677**

**June 2014**

## **NOTICES**

### **Disclaimers**

The findings in this report are not to be construed as an official Department of the Army position unless so designated by other authorized documents.

Citation of manufacturer's or trade names does not constitute an official endorsement or approval of the use thereof.

Destroy this report when it is no longer needed. Do not return it to the originator.

# **Army Research Laboratory**

Adelphi, MD 20783-1197

---

---

**ARL-TR-6677**

**June 2014**

---

## **The Integrated Distributed Virtual Research Network: An Introduction**

**Colleen Adams**

**Computational and Information Sciences Directorate, ARL**

REPORT DOCUMENTATION PAGE				Form Approved OMB No. 0704-0188	
<p>Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.</p> <p><b>PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.</b></p>					
1. REPORT DATE (DD-MM-YYYY) June 2014		2. REPORT TYPE Interim		3. DATES COVERED (From - To) 1/2012–8/2013	
4. TITLE AND SUBTITLE The Integrated Distributed Virtual Research Network: An Introduction				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) Colleen E. Adams				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) U.S. Army Research Laboratory ATTN: RDRL-CIH-N 2800 Powder Mill Road Adelphi, MD 20783-1197				8. PERFORMING ORGANIZATION REPORT NUMBER  ARL-TR-6677	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)  ARL	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited.					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT <p>The Integrated Distributed Virtual Research Network (IDVRN) is the U.S. Army Research Laboratory's (ARL) Research, Development, Test and Evaluation Network. It provides ARL researchers and their remote external partners the capabilities to collaboratively conduct research within secure virtual enclaves. Research may include use of hardware and/or software resources that could not be used on ARL's enterprise network due to Information Assurance restrictions. A secure research enclave and its authorized membership can be established in a timely, cost-efficient manner. This interim report provides an introduction to IDVRN and the capabilities it provides. A background section describes the progression from the recognition of need in the mid-2000s to the current state. An overview of IDVRN's operational environment is provided, and the types of external connections allowed are described. The process for establishing an enclave is outlined. Responsibilities of the various ARL entities involved with IDVRN are defined.</p>					
15. SUBJECT TERMS IDVRN					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT  UU	18. NUMBER OF PAGES  28	19a. NAME OF RESPONSIBLE PERSON Colleen Adams E.
a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified			19b. TELEPHONE NUMBER (Include area code) (301) 394-4640

---

## Contents

---

<b>List of Figures</b>	<b>v</b>
<b>Acknowledgments</b>	<b>v</b>
<b>Preface</b>	<b>vi</b>
<b>1. Introduction</b>	<b>1</b>
1.1 The ARL Enterprise Network (ARLEN) .....	1
1.2 Need for a Research and Development Network .....	1
<b>2. Background</b>	<b>2</b>
<b>3. Operational Environment Overview</b>	<b>4</b>
<b>4. Connectivity Allowed</b>	<b>5</b>
4.1 Extended Enclaves .....	5
4.2 Intra-Enclave .....	6
4.3 Inter-Enclave .....	6
4.4 Enclave-to-Internet .....	7
4.5 Open ARLEN User to Enclave Via Approved Ports, Protocols and Services (PPS).....	7
4.6 External User to Enclave Via RVPN .....	7
4.7 External User to Internet-Facing Server in the IDVRN IFS DMZ .....	8
4.8 Enclave to Open ARLEN (Highly Restricted) .....	8
<b>5. Process for Establishing an Enclave</b>	<b>8</b>
<b>6. Operational Responsibilities</b>	<b>9</b>
6.1 The HPCNB .....	9
6.2 The Enclave Proponent .....	10
6.3 The Information Assurance Management Office .....	10
6.4 The IDVRN CCB .....	11
<b>7. Authority to Operate</b>	<b>11</b>

<b>8. References</b>	<b>12</b>
<b>Appendix A</b>	<b>13</b>
<b>Appendix B</b>	<b>15</b>
<b>Distribution List</b>	<b>17</b>

---

## List of Figures

---

Figure 1. ARL VPN mesh.....	1
Figure 2. IDVRN logical structure.....	5
Figure 3. IDVRN external connectivity allowed. ....	6

---

## Acknowledgments

---

Thanks to Dr. Raju Namburu, Chief, Computational Sciences Division, for his leadership and support, without which the Integrated Distributed Virtual Research Network (IDVRN) would not have become the valued resource it is for ARL.

Thanks to Mr. Charlie Nietubicz, former Chief, Advanced Computing and Computational Sciences Division, for his help in getting IDVRN off the ground.

Special thanks to Dr. Windell Ingram, Tom Kile, Theron Trout, and Gary Cohn for their extensive contribution to this document to include reviews, comments, and edits, which contributed to the quality of the document.

The ARL Integrated Distributed Virtual Research Testbed (IDVRT) team, consisting of Alex Tarantin, Khoa Bui, Tom Kile, Jeanne Angelini, Dr. Loretta Moore, Dr. Adrienne Raglin, Dr. Alan Wetmore, and Leelinda Parker, deserves special recognition for its groundbreaking work. Although Information Assurance regulations did not adequately address research networks, the IDVRT Team persisted and produced a testbed that served the ARL R&D community well, and satisfied the ARL IAM and the DAA. As a result, the testbed evolved to become ARL's research network, IDVRN.

Thanks to Cem Karan, who volunteered to stand up the first proof-of-concept IDVRT enclave for the Blue Radio project. His enthusiastic and untiring support contributed much to an early success story, without which IDVRT would have faced an uncertain future.

Thanks to the team that conducted the CISD Leadership Institute's Capstone Project called Enclave-Based Research Networks, which also contributed greatly to the success of IDVRT. The team consisted of Barry O'Brien, Natalie Ivanic, Richard Gopaul, Alan Wetmore, Michael Lee, Nathan Boyer, Mark Thomas, Tim Hanratty, and Anthony Thomas.

Thanks to former ARL IAM Stan Niles and the ARL ACA Curtis Arnold, who supported IDVRT and IDVRN from the beginning.

Lastly, thanks to Patricia Camacho, who assisted with publication.



---

## Preface

---

This report provides an introduction to the Integrated Distributed Virtual Research Network (IDVRN), and the capabilities it provides to ARL researchers and their collaborators. A background section describes the progression from the recognition of need in the mid-2000s to the current state. An overview of IDVRN's operational environment is provided, and the types of external connections allowed are described. The process for establishing an enclave is outlined; details will be provided in forthcoming on-line documents. Responsibilities of the various ARL entities involved with IDVRN are defined. This report is intended to be useful to:

- the High Performance Computing Networking Branch (HPCNB) staff;
- members of the IDVRN Configuration Control Board (CCB);
- the ARL Information Assurance Management (IAM) office;
- security reviewers;
- ARL scientists and engineers who are proponents of established IDVRN enclaves and those interested in establishing an enclave;
- enclave members;
- ARL managers and executives; and
- other Army organizations interested in establishing Research, Development, Test and Evaluation (RDT&E) networks.

A Concept of Operations report will follow; it will detail IDVRN's management and usage policies, and describe its security policies and security architecture.

INTENTIONALLY LEFT BLANK.

---

## 1. Introduction

---

### 1.1 The ARL Enterprise Network (ARLEN)

The ARLEN is an integrated Virtual Private Network (VPN) mesh serving six ARL locations, as shown in figure 1. The ARLEN provides secure, reliable, high-speed data-communications within the ARL community. VPN connectivity is provisioned over the Defense Research and Engineering Network (DREN) wide-area-network (WAN) service. The WAN bandwidth provided to the different sites ranges from DS3 (45 Mbps) to OC48 (2.4 Gbps). Each site is part of the ARLEN VPN and also has a direct connection to DREN. There are also managed cross-connections to the NIPRNet, which are managed by the Network Enterprise Center (NEC) at each site. The High Performance Computing Networking Branch (HPCNB) designs, installs, manages, and maintains the ARLEN at all ARL sites (See appendix A for the HPCNB organization chart).

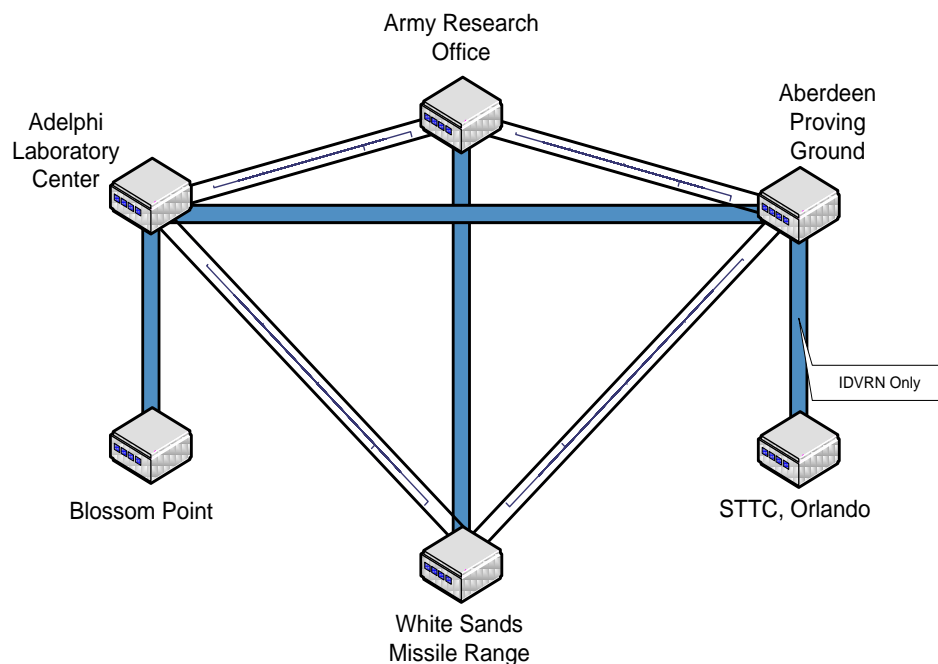


Figure 1. ARL VPN mesh.

### 1.2 Need for a Research and Development Network

The ARLEN is a DREN enclave and, thus, accommodates some R&D activities that could not be conducted on an operational network, e.g., the NIPRNet. However, not all R&D work can be conducted on the open ARLEN. The ARLEN as a whole serves the entire ARL community and must not be exposed to R&D activities that carry elevated information assurance (IA) risks. Many ARL R&D projects—especially experimental development (6.2) and customer projects—

require experimental systems that carry such risks. To accommodate such systems, some ARL groups established research networks that were private and physically isolated from the ARLEN. This solved some of their problems but created others. These isolated networks could not access any email system or the Internet, and had no efficient means to share resources or data with collaborators who were not connected to the local isolated network. Lack of Internet access made it difficult and time-consuming to transfer patches and security hot-fixes to computers within the isolated networks. Use of such networks also created the need for many researchers to have two office computers, one connected to the ARLEN and the other connected to their research network.

Much of ARL's R&D is conducted in collaboration with external partners (e.g., universities, industry, other government agencies (OGAs)), who execute a substantial part of ARL's R&D program. Sharing access to experimental systems is often essential to this collaboration. However, collaborating partners cannot access the ARLEN. To enable such collaboration, some research groups chose to outsource the computing and networking resources needed for their research—i.e., they established laboratories or outposts at contractor sites that ARL researchers and external collaborators could access via the Internet.

Neither totally isolated networks nor the outsourcing of resources provided a satisfactory solution. Isolated networks exclude or impair collaboration, and outsourcing removes key R&D resources from the control of ARL while exposing them to increased risk from potential IA vulnerabilities that would be mitigated or corrected were the resources at ARL. Thus, there is a clear need for an ARL-hosted R&D network that can accommodate elevated-risk activities and can be shared among internal and external collaborators. IDVRN satisfies this need. While ARL was the first Army organization to develop such a network (see section 2), ARL is no longer alone. Indeed, the Army has recognized the need for robust RDT&E networks (6) that do not put operational networks at risk. Other Army organizations are also pursuing such networks (7).

---

## **2. Background**

---

Due to the increasing threat of cyber attacks over the last decade, DoD and the Army have pushed to enforce rigorous IA policies that have had a restrictive effect on the capabilities that had previously been available to researchers using the ARLEN. Increasingly, researchers encountered IA roadblocks that could not be overcome—roadblocks that severely hampered in-house research at ARL. As a result, some groups took the approaches described in section 1.2, i.e., using physically disconnected research networks and/or outsourcing. ARL research proponents, both in and outside the HPCNB, believed that research networks based on firewall-separated, VLAN-defined enclaves within the physical infrastructure of the ARLEN offered a better, more cost-effective solution. They identified technologies that provided a network of enclaves that allowed well-controlled access to authorized users, both internal and external to

ARL, while maintaining the security of both the ARLEN and the enclaves. However, lack of IA guidance for such networks proved to be a major obstacle.

In 2006, the HPCNB formed the High Performance Computing (HPC) Network Applied Research Team with the goal of developing and executing an experimental development plan to advance the state of high-performance wired networking at ARL. It was envisioned that such advances might also benefit the Army and the DoD, particularly the DREN.

That same year, the Integrated Distributed Virtual Research Testbed (IDVRT) (*1*) team was established to address the requirement for an ARL research network that facilitates R&D that entails elevated IA risks and/or requires collaboration with external partners. A goal was to take advantage of the existing physical infrastructure of the ARLEN rather than creating a separate physical network. The team included personnel from the Network Applied Research Team, researchers from the Battlefield Environment Division (BED), and the Chair of the Computer Science Department at Jackson State University. IDVRT objectives included:

- creating several virtual enclaves to accommodate R&D needs of different ARL projects or organizations;
- assessing and resolving issues related to different types of enclaves;
- establishing a well-defined technical process for creating and maintaining enclaves;
- exploring with the ARL IAM means to simplify and standardize the IA approval process; and
- gaining approval for offering IDVRT enclaves as a standard service of the HPCNB.

A technical plan was developed, along with network policies and mechanisms intended to allow research to be conducted on the IDVRT while maintaining the security and integrity of both the ARLEN and the IDVRT. The first enclave established and used as a proof of concept for security and usability was the Blue Radio project, and several others followed soon after.

While the development of the IDVRT was underway, a CISD Leadership Institute Capstone Project called Enclave-Based Research Networks (the Capstone Project) was also exploring the feasibility of such a research network. To members of the Capstone Project team, the IA approval process to establish such networks was initially unknown and proved to be daunting. The IA staff at ARL had no experience with such a network, and DoD and Army regulations did not fully address the need. The Capstone team found a collaboration partner in the IDVRT team, and both the Capstone Project and IDVRT benefitted from the partnership. Indeed, IDVRT was to become the mechanism that solved the problems encountered by the Capstone Project.

From the IDVRT and Capstone Project experiences (*4*), it was learned that:

- commercial networking technologies are sufficient for the isolation & security required for the enclaves;

- the IA approval process could be straightforward and timely using an approved process with good documentation;
- routinely gaining approval for enclaves would require the process be followed consistently, which would require an IDVRT coordinator within HPCNB; and
- for IDVRT services to work well and satisfy customers, they would require technical support staff proficient in not only the technologies employed, but also the intent of IDVRT, how it must function to serve customers, and the security issues and IA process.

As a result of technical success and positive feedback from enclave customers, IDVRT was approved by the IAM and DAA to be a standard ARL service (2, 3) and renamed the Integrated Distributed Virtual Research Network (IDVRN) to replace the “testbed” designation.

As the HPCNB gained experience operating IDVRN and the number of enclaves grew, improvements were made including:

- adding more methods to access an enclave
- adding more security mechanisms
- better defining capabilities, policies, and restrictions

This upgraded IDVRN is the focus of the remainder of this report.

---

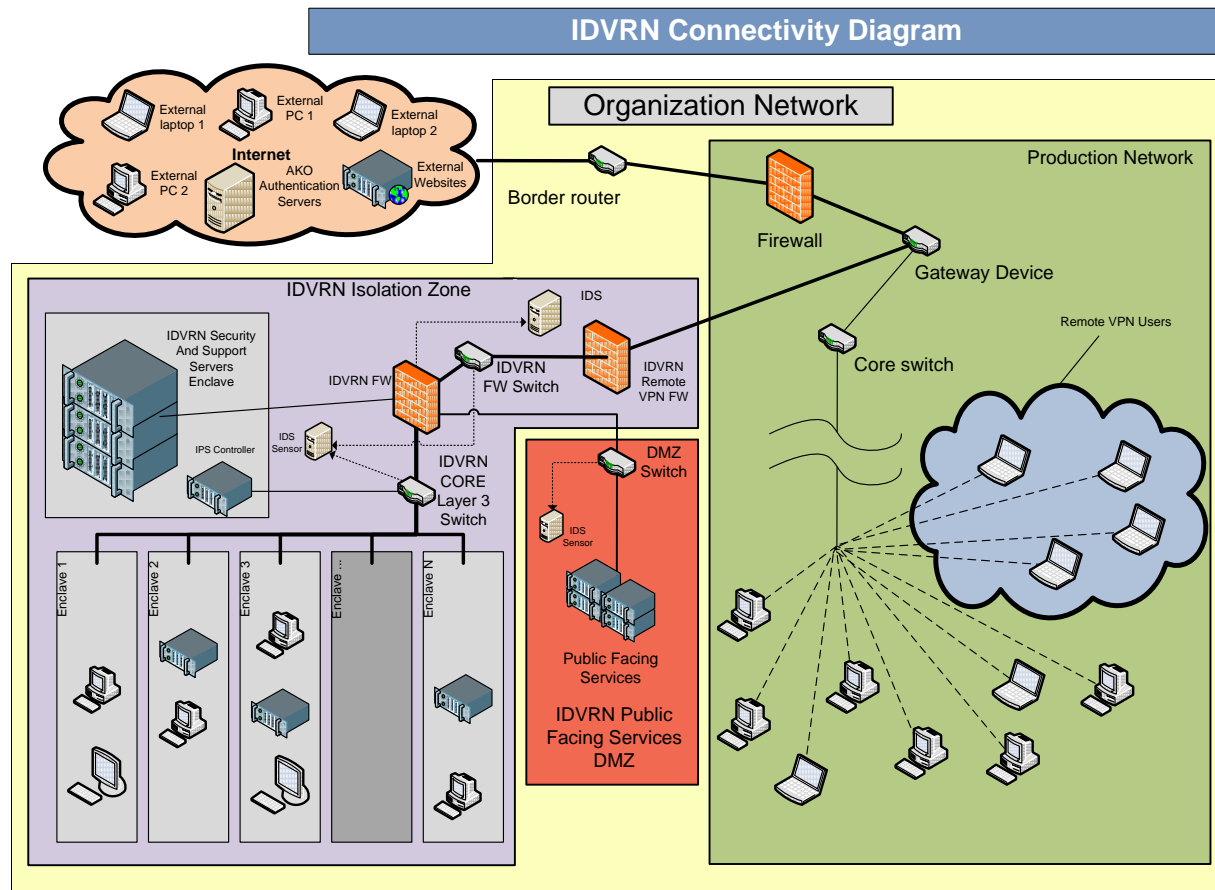
### **3. Operational Environment Overview**

---

IDVRN comprises a set of virtual enclaves, each with boundaries defined by its own Virtual Local Area Network (VLAN) edges and firewall policies. Each enclave is isolated from both the open ARLEN and other enclaves, and each is accessible by only its enclave members, both internal and external to ARL. This isolation helps to achieve one of the most fundamental principles of IDVRN in that it must not harm the ARLEN. Accordingly, the open ARLEN treats IDVRN as an untrusted Internet site, with controlled exceptions. An enclave may include servers, PCs, instruments, and experimental equipment as needed by the project(s) supported by the enclave. Within the constraints of the IDVRN Acceptable Use Policy (AUP) and Non-Disclosure Agreement, each enclave proponent (an ARL employee requesting and taking responsibility for the enclave) has responsibility and authority for approving enclave membership and granting elevated privileges to members as necessary to conduct their R&D. Enclave security is administered by a trained and certified System Administrator (SA) provided by the enclave proponent.

Figure 2 provides a high-level depiction of the networking of IDVRN at ALC. Similar configurations are in place at other ARL sites. Since a primary goal of IDVRN is to allow

elevated-risk systems to operate within an enclave, the focus of security is risk mitigation through a variety of policies and mechanisms including stringent boundary security, both at the IDVRN boundary and at each enclave boundary.



Revision 1, 2012-08-07

Figure 2. IDVRN logical structure.

## 4. Connectivity Allowed

Figure 3 depicts all the types of external connectivity allowed by IDVRN. The following types of connectivity may be provided as needed.

### 4.1 Extended Enclaves

As shown in figure 3, an enclave can be extended via permanent VPN to include systems belonging to and residing with all categories of enclave members:

- ARL members at any ARL site, with enclave systems located in their offices or lab areas

- Army/DoD/OGA partners, with enclave systems located in their physical areas at any site with Internet access
- university/industry partners, also unrestricted regarding location

Systems at these extended enclave locations are not “accessing an enclave” as an external system; they are part of the enclave and are treated as such by IDVRN control components.

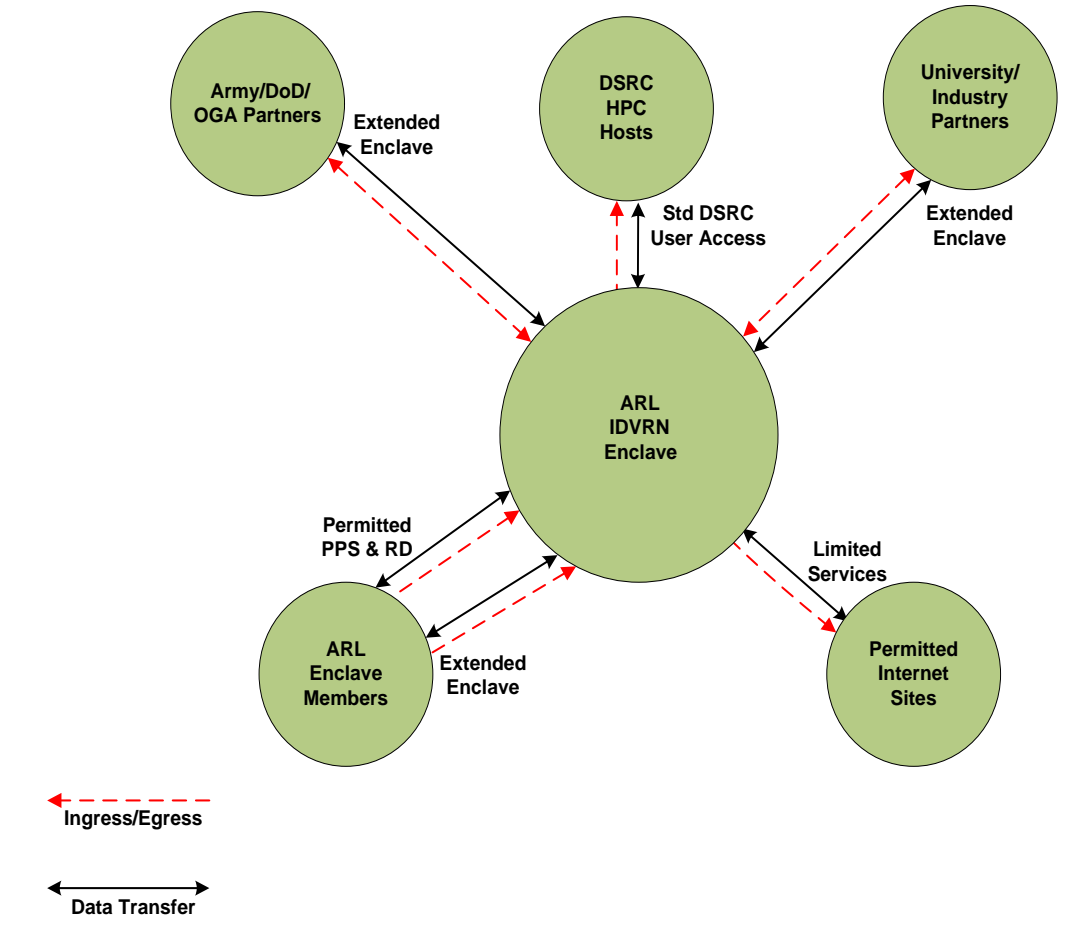


Figure 3. IDVRN external connectivity allowed.

## 4.2 Intra-Enclave

IDVRN policies put no restrictions on intra-enclave traffic that does not have a negative impact on other network operations. The enclave proponent may choose to permit or deny an enclave member access to any enclave system by issuing them accounts on only those systems that they may access.

## 4.3 Inter-Enclave

If more than one enclave belongs to the same proponent, the proponent is free to decide the policy regarding inter-enclave connectivity. If two or more enclave proponents wish to establish



inter-enclave connectivity, they must agree on the permissions and restrictions on that connectivity. As a good practice, enclave proponents should evaluate compatibility of enclave policies (e.g., compatible user restrictions) when determining what inter-enclave communication is appropriate. As a policy, each enclave proponent must disclose his/her enclave members to proponents of interconnected enclaves. Inter-enclave connectivity is controlled by the IDVRN firewall. The HPCNB will configure the IDVRN firewall to provide connectivity as requested by the enclave proponent(s); no inter-enclave connectivity is the default.

#### **4.4 Enclave-to-Internet**

Connections from IDVRN to the Internet carry more restrictions than are applied to ARLEN-to-Internet connections. Some controls are, in fact, applied to traffic that traverses any DoD network. All are limited by the approved set of ports, protocols, and services as defined by the DoD Ports, Protocols, and Services Management (PPSM) guidance (10). IDVRN restrictions are enforced by the IDVRN firewall using a deny all, permit by exception (DAPE) policy. As shown in Figure 3, access to a High Performance Computing (HPC) system at a Defense Supercomputer Resource Center (DSRC) by an enclave member having a valid DSRC user account and authority to use said system will be permitted.

#### **4.5 Open ARLEN User to Enclave Via Approved Ports, Protocols and Services (PPS)**

An IDVRN enclave poses no more risk to the open ARLEN than does the Internet. Thus, an enclave's members' connections from the open ARLEN to their enclave are limited by the same rules that are applied to their connections from the ARLEN to the Internet. That is, IDVRN members' ARLEN PCs will be allowed to communicate with their enclave using PPS as limited by the PPSM guidance. (PPS not approved by the PPSM guidance may be permitted with IAM approval.) The IDVRN firewall will enforce the PPSM rules, again using a DAPE policy, and will assure member-only access based on the static IP addresses assigned to members' PCs. The enclave proponent may choose to restrict which members have enclave access from the open ARLEN and/or which enclave systems are accessible from the open ARLEN.

#### **4.6 External User to Enclave Via RVPN**

The RVPN software allows an enclave member's external computer to temporarily connect to and become part of the member's enclave. RVPN client software is configured to contain the user's enclave credentials, including its assigned IP address pool. When a connection is initiated by the client, the IDVRN RVPN firewall verifies both the user's SecurID and enclave credentials. The remote computer is assigned an IP address reserved for the member's enclave. Encrypted traffic flows between the client and the IDVRN RVPN firewall. The RVPN firewall sends traffic either to the enclave, via the IDVRN Firewall, or to the Internet, also via the IDVRN Firewall. The enclave proponent may choose to limit the access rights of certain systems connected via RVPN. Any such restrictions will be enforced by the IDVRN Firewall, which will

be configured by the HPCNB. Outbound Internet traffic from an RVPN-connected system is filtered in the same manner as is traffic from other permanently connected enclave systems.

#### **4.7 External User to Internet-Facing Server in the IDVRN IFS DMZ**

Direct connections from external sites to normal IDVRN systems are not permitted, and in some cases, it may not be feasible for external members to connect to their enclave via a permanent enclave extension or by using RVPN. For example, this may be the case for external Army or DoD users. In other cases, the enclave proponent may want to limit some external users to a single application or service. To satisfy such needs, a server may be set up in the IDVRN Internet-facing servers (IFS) DMZ (figure 2) to provide external enclave members with Internet-facing services that can access back-end services within the member's enclave. An IFS DMZ server may access resources inside the server's IDVRN enclave that are required to fulfill its function (access a database server, for example). Access to Secure Sockets Layer (SSL)/Transport Layer Security (TLS)-enabled services will be restricted to users with a CAC or HPCNB-issued client certificate. Each user of this capability will be limited by the server's user-configuration to only those services authorized for the user by the enclave proponent. With IAM approval, a publically accessible service may be deployed within the IDVRN IFS DMZ that does not require user-level authentication or authorization.

#### **4.8 Enclave to Open ARLEN (Highly Restricted)**

Protection of the open ARLEN from ingress by outsiders is an essential security requirement of IDVRN and, thus, this type of access must be guarded very carefully. Access to DNS and KDC servers in the open ARLEN by their respective client programs is permitted only when access is established and controlled by the enclave's Trained & Certified SA. Any ARLEN servers not open to access from the Internet will not be accessible from IDVRN enclaves without IAM approval.

---

### **5. Process for Establishing an Enclave**

---

More details of the process outlined here will soon be available from the HPCNB, as will templates of the documents referenced.

- First, the enclave proponent contacts the HPCNB to request an enclave. An HPCNB representative collaborates with the proponent to plan and design the enclave and document specifics of the enclave requirements and costs. Both parties sign the requirements document. Copy is provided to IAM for approval.
- IAM approves the request or sends it back for clarification/revision.

- If a new enclave has unusual or previously unaddressed requirements that necessitate an architectural or policy change within IDVRN, Configuration Control Board (CCB) approval may be required prior to enclave implementation.
  - The enclave proponent signs an IDVRN Certificate of Non-Disclosure that certifies that all enclave members are need-to-know collaborators, understand restrictions on dissemination of information, such as FOUO, and conform to such restrictions. The proponent must assure that prior to any public release, information from his/her enclave is processed properly, via ARL Form 1, whether release is by ARL or external partners. The proponent also accepts responsibility for acquisition, operation, and maintenance of all systems within the enclave.
  - As an enclave user, the proponent signs the IDVRN Acceptable Use Policy (AUP) Agreement for ARL Users. This AUP is derived from the ARL-standard AUP and tailored specifically for ARL's IDVRN users.
  - Each enclave member signs an AUP Agreement tailored for IDVRN. Internal ARL enclave members sign the IDVRN AUP Agreement for ARL Users and external, non-ARL enclave members sign the IDVRN AUP Agreement for Non-ARL Users. In each case, the member agrees to take responsibility for safeguarding the information contained within his/her enclave.
  - Each enclave member who will use SecurID for authentication must request and be issued a SecurID card prior to accessing the enclave.
  - The Trained and Certified SA assigned to the enclave performs initial configuration management and Baseline Security functions on all enclave systems.
  - The HPCNB configures the networking equipment to establish the enclave's network as required by the proponent's request.
  - The HPCNB notifies the proponent that the enclave is operational.
- 

## **6. Operational Responsibilities**

---

### **6.1 The HPCNB**

The HPCNB is responsible for:

- producing, in collaboration with the enclave proponent, the requirements document needed to establish an enclave;

- creating and maintaining the IDVRN network infrastructure including the configuration of all switches and firewalls to provide the required enclave isolation, routing, encryption and decryption, user authentication, and IP filtering;
- securing the IDVRN boundary and the boundary of each enclave;
- consulting with the IDVRN (CCB) and the IAM as necessary; and
- providing the CCB and/or the ARL IAM with IDVRN reviews and updates as may be required.

## **6.2 The Enclave Proponent**

The enclave proponent must oversee and assign responsibility for:

- collaborating with the HPCNB to plan the enclave and define its technical requirements;
- submitting his/her Certificate of Non-Disclosure and the Acceptable Use Policy (AUP) statements for all enclave members;
- controlling the enclave membership and vouching for each member;
- acquiring, maintaining, and operating all systems within the enclave;
- providing a trained and certified SA for the enclave;
- documenting systems and non-standard software used in the enclave;
- documenting deviations from standard security practices needed to conduct research;
- maintaining security awareness among enclave users; and
- all other enclave duties not related to networking or enclave boundary security.

## **6.3 The Information Assurance Management Office**

The IAMO is responsible for:

- approving each valid request for a new enclave;
- approving requests for the use of non-standard operating systems;
- approving requests from enclave proponents to deviate from the security baseline for IDVRN systems;
- approving requests to establish internet-facing services in the IDVRN IFS DMZ, including public services—i.e., those that do not require authentication or authorization to access; public services must also be approved by the ARL Public Affairs Office (PAO);
- approving requests to use non-PPSM approved transport protocols within the IDVRN IFS DMZ;

- approving requests for access to specific servers and/or services on the open ARLEN from an IDVRN enclave;
- assisting in reviewing proposed changes to IDVRN policies, mechanisms, and practices prior to IDVRN CCB decision; and
- participating in the IDVRN CCB.

#### **6.4 The IDVRN CCB**

The CCB is responsible for:

- approving proposed changes to IDVRN policies, mechanisms, and practices; and
  - reporting to the ARL Enterprise Configuration Control Board (AECCB) all of its decisions and actions pertaining to IDVRN.
- 

### **7. Authority to Operate**

---

A memorandum requesting Authority to Operate IDVRT (renamed IDVRN) was formally approved by the ARL DAA in 2007 (1, 2), and IDVRN has been included in all subsequent ARL ARLEN DIACAPs. A memorandum updating the authority for IDVRN, version 2 was approved by the ARL DAA in 2012 (5).

---

## 8. References

---

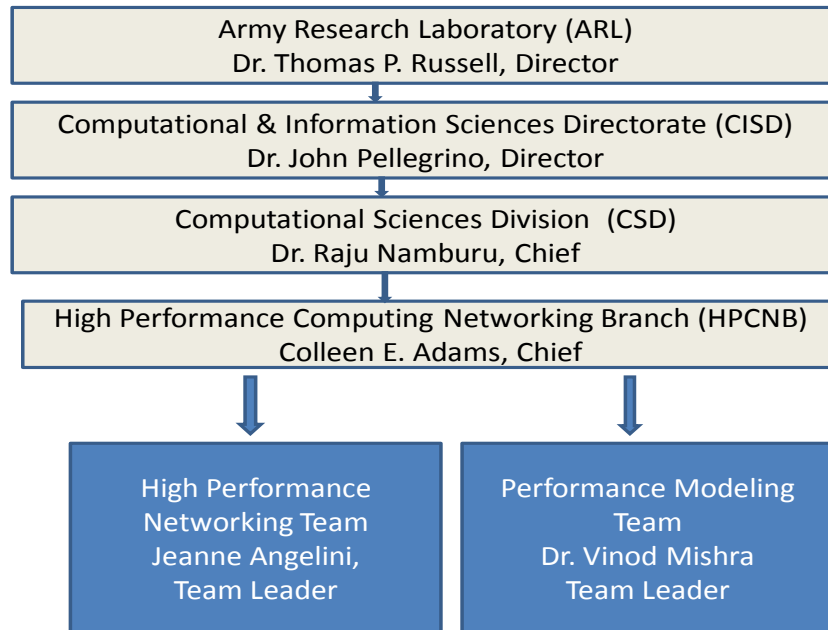
1. Memorandum, AMSRD-ARL-CI-HN, 27 June 2007, Setting Up an Integrated Distributed Virtual Research Testbed (IDVRT).
2. Memorandum, AMSRD-ARL-CI-O, 3 August 2007, Review and Update to the Army Research Laboratory Enterprise Network (ARLEN) System Security Authorization Agreement (SSAA).
3. Proposal, 18 September 2007, The Establishment of an Integrated Distributed Virtual Research Testbed.
4. O'Brien, Barry et al. *Enclave-Based Research Networks, CISD Leadership Institute Capstone Project Final Report*; ARL-TR-4141; U.S. Army Research Laboratory: Adelphi, MD, June 2007.
5. Memorandum, AMSRD-ARL-RDRL-CIH-N, 15 February 2012, Continued Operation of the Integrated Distributed Virtual Research Network (IDVRN).
6. Research, Development, Test & Evaluation (RDT&E) Networks, Information Assurance Certification & Accreditation (IA C&A) Requirements (Draft), 20 April 2010, Department of Army, G6-CIO, Best Business Practices (BBP).
7. A Proposal for Management of and Service Delivery to the ERDC Research and Development Environment, 16 April 2010, U.S. Army Engineer Research and Development Center.
8. Blog Entry, November 2011, Hacking HP Printers for Fun and Profit, John Bambenek, <http://isc.sans.edu/diary.html?storyid=12112>
9. Department of Defense Enclave Security Technical Implementation Guide, 28 January 2011.
10. Ports, Protocols, and Services Management (PPSM), <http://iase.disa.mil/ports/index.html>

---

## Appendix A

---

### HPCNB Organization Structure



INTENTIONALLY LEFT BLANK.



---

## Appendix B

---

RDRL-CIH

5 May 2013

### MEMORANDUM FOR RECORD

SUBJECT: US Army Research Laboratory (ARL) Interim RDT&E Network Configuration Control Board (ROT&EN CCB) Charter

1. Name of Committee: ARL RDT&EN Configuration Control Board (ARDT&EN CCB).
2. Duration: This Charter is effective immediately and terminates upon direction of the ARL Corporate Information Officer.
3. Category and Type of Committee/Scope: The ARDT&E Network Configuration Control Board will focus on IDVRN and in the future will manage similar entities.
4. Purpose: The ARDT&EN CCB will review and approve or disapprove all proposed changes to the policies, mechanisms and practices of operation of the IDVRN, ARL's ROT&E network.
5. Membership:
  - a. Chief, High Performance Networking Branch (Chair-voting member) Colleen Adams
  - b. Deputy CIO (voting member) Rudy Mazariegos
  - c. ARL Information Assurance Manager (IAM) (voting member) Janet Churchwell
  - d. Chief, Battlefield Information Processing Branch (voting member) Larry Tokarcik
  - e. Chief, Information Management Branch (voting member) Rose King
  - f. Chief, ISR Technology Integration Branch (voting member) Dr. Andrew Ladas-SEDD
  - g. Chief, Cognitive Sciences Branch (voting member) Dr. Don Headly-HRED
  - h. Researcher Representative, Multilingual Computing (voting)- Dr. Reggie Hobbs CISD
  - i. Researcher Representative, Atmospheric Sensing Branch (voting)- Dr. Alan Wetmore CISD J.
  - j. Researcher Representative, Ground Combat Branch (voting)- Dr. Jeffrey Smith- SLAD
  - k. Researcher Representative, Guidance Navigation, Control, Guide Technologies (voting) – Dr. Mark ILG - WMRD
  - l. Researcher Representative, Computing Architectures Branch (Branch Chief) (non-voting member) Dale Shires (CISD)
  - m. Researcher Representative, Operations Group-Orlando, (non-voting member) Mark Brzezinski-HRED
  - n. Network Engineer (non-voting member) Tom Kile
  - o. Network Engineer (non-voting member) Theron Trout
  - p. Non-voting members (serving at the invitation of the Chair)
6. Direction and Control: The ARDT&EN CCB is subordinate to the ARL Enterprise Configuration Control board (AECCB) and will report all ARDT&EN decisions and actions to that board.

RDRL-CIH

SUBJECT: US Army Research Laboratory (ARL) Interim RDT&E Network Configuration Control Board (ROT&EN CCB) Charter

7. Voting and Substitutes: All voting members will have an equal vote and may send substitutes with proxies. Meetings will follow an agenda, with open discussion of each topic. Robert's Rules of Order will not be strictly followed. The Chair will strive for consensus. Subject matter experts will be invited as needed and will have a voice, but not a vote.

8. Roles and Responsibilities: The Chief, High Performance Networking Branch will Chair the ARDT&EN CCB.

a. Chair:

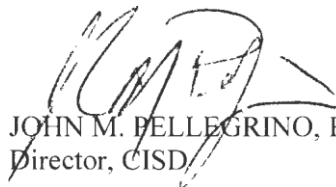
- (1) Provides oversight and guidance.
- (2) Provides coordination.
- (3) Ensures the voice of all members and interested stakeholders is heard.
- (4) Keeps the charter current.
- (5) Prepares and publishes agendas and minutes.
- (6) Presides at meetings and maintains order.
- (7) Publishes final decisions.
- (8) Implements approved changes.

b. Members:

- (1) Review and evaluate proposed changes prior to meetings.
- (2) Discuss proposed changes in meetings.
- (3) Vote on proposed changes (voting members only).
- (4) Support the decisions of the ARDT&EN CCB.

9. Schedule: Meetings will be called by the Chair when needed. Attendance may be in person or via electronic means. Issues may be discussed and voted on via electronic means, including email.

10. Point of Contact for this memorandum is Colleen Adams, (301) 394-4640.



JOHN M. PELLEGRINO, Ph.D.  
Director, CISD

1 DEFENSE TECHNICAL  
(PDF) INFORMATION CTR  
DTIC OCA

2 DIRECTOR  
(PDFS) US ARMY RESEARCH LAB  
RDRL CIO LL  
IMAL HRA MAIL & RECORDS MGMT

1 GOVT PRINTG OFC  
(PDF) A MALHOTRA

1 US ARMY RESEARCH LAB  
(PDF) RDRL CIH N  
COLLEEN E. ADAMS

INTENTIONALLY LEFT BLANK.